EXPRESS MAIL LABEL NO.: EL863782985US

ABSTRACT OF THE DISCLOSURE

FLEXIBLE GALOIS FIELD MULTIPLIER

A flexible Galois Field multiplier is provided which implements multiplication of two elements within a finite field defined by a degree and generator polynomial. One preferred embodiment provides a method for multiplying two elements of a finite field. According to the method, two input operands are mapped into a composite finite field, an initial KOA processing is performed upon the two operands in order to prepare the two operands for a multiplication in the ground field, the multiplication in the ground field is performed through the use of a triangular basis multiplier, and final KOA3 processing and optional modulo reduction processing is performed to produce the result. This design allows rapid redefinition of the degree and generator polynomial used for the ground field and the extension field.

230-A01-007